AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Manuel d'installation
De la Cryptolib CPS
Dans un environnement client/serveur
TSE/CITRIX

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. + 33 (0)1 58 45 32 50
www.asipsante.fr
Agir ensemble pour soigner mieux

Sommaire

1 Contexte 3
2 Configuration requise 4
3 Description de l'installation (version GALSS).... 5
3.1 Déroulement.....5
3.2 Vérification du bon fonctionnement de la cryptolib 6
3.3 Paramétrage.....6
4 Description de l'installation (version PC/SC) ... 8
4.1 Déroulement.....8
4.2 Paramétrage.....8
5 Emplacements des fichiers 9
5.1 Chemin d'accès profil utilisateur [USER] 9
5.2 Version GALSS.....10
5.3 Version PC/SC.....10
6 Annexe..... 11
6.1 Commande « change user » 11
Syntaxe.....11
Paramètres.....11
Remarques.....11
6.2 Commande « change port » (changer le port).....12
Syntaxe.....12
Paramètres.....12
Remarques.....12

Copyright ASIP Santé 2011. Tous droits réservés.

1 Contexte

Ce document complète le manuel d'installation de la cryptolib CPS standard en précisant la procédure d'installation particulière pour les environnements client/serveur type TSE/CITRIX.

Cette procédure concerne:

- la Cryptolib CPS sur architecture GALSS **:** **CryptolibCPS-04.XX.XX.msi** (ce setup n'installant pas le GALSS, celui-ci doit d'abord être installé à partir du setup GALSS : **galss-3.XX.XX.msi**)

(Au minimum, la version 3.32 du GALSS est recommandée pour une utilisation en environnement TSE/CITRIX)

- la Cryptolib CPS sur architecture PC/SC : **setupCryptoCpsPcsc.vX.XX.msi** (sans GALSS)

Copyright ASIP Santé 2011. Tous droits réservés.

2 Configuration requise

Ce document décrit la procédure d'installation pour les machines serveur fonctionnant sous les systèmes d'exploitation Windows suivants :

- ✓ Windows 2003 Server (32 et 64 bits)
- ✓ Windows 2008 Server (32 et 64 bits)

Et ayant le rôle « Terminal Server » (TSE) installé sur le système.

Remarque :

- En environnement 64 bits, les Cryptolibs actuelles fonctionnent en mode émulation 32 bits. Les applications utilisées ne peuvent donc être que des applications 32 bits (navigateurs, clients de messagerie, …). De même, le mécanisme de « SmartCardLogon » mis en œuvre de manière native par le système ne fonctionne pas sur un système 64 bits du fait de cette émulation.

=> L'installation de la Cryptolib CPS se fait exclusivement sur le serveur. Aucun composant CPS n'a besoin d'être installé sur les postes client.

=> Lors de l'installation de la Cryptolib CPS version GALSS, le serveur devra disposer préalablement d'au moins un lecteur de carte (PC/SC ou PSS) présent et correctement installé sur le poste.

(sinon la procédure d'installation du GALSS ne pourra se terminer correctement)

=> Si le serveur tourne dans un environnement virtualisé (type VMware, Hyper-V, XenServer, …), c'est sur le poste client pilotant le serveur (utilisateur avec les droits administrateur), que devra être présent le lecteur de cartes (et pas sur la machine où est hébergé physiquement le serveur).

Copyright ASIP Santé 2011. Tous droits réservés.

3 Description de l'installation (version GALSS)

3.1 Déroulement

Vous devez être administrateur du serveur (avoir tous es droits d'écriture et d'accès), avant de démarrer la procédure.

1/ Passage en mode « installation » du serveur :

En ligne de commandes, lancer la commande : **change user /install**

(Voir « Annexe »).

2/ Lancer le setup d'installation de la Cryptolib CPS sur GALSS pour Windows.

Suivre ensuite le déroulement de l'installation comme indiqué dans le manuel d'installation standard de la cryptolib CPS GALSS.

A la fin de l'installation, le setup vous demandera de redémarrer votre serveur (pour la version GALSS de la cryptolib).

3/ Passage en mode « exécution » du serveur :

En ligne de commandes, lancer la commande : **change user /execute**

(Pour vérifier en quel mode le serveur se trouve, lancer la commande **change user /query**)

4/ Déplacer les 2 fichiers .INI de la cryptolib (**galss.ini** et **cps_pkcs11_safe.ini**) du répertoire Windows (« **C:/Windows** » par défaut), vers le sous-répertoire \Windows du répertoire de base de l'utilisateur (« **C:/documents and settings/ «utilisateur» /Windows** »)

Important : Bien vérifier que ces deux fichiers ne sont plus présents dans le répertoire Windows (« **C:/Windows** » par défaut)

Remarque : dans le cas où le setup est exécuté sur le serveur, sans être passé en mode « installation », tous les fichiers seront copiés dans le répertoire de base de l'utilisateur (« **C:/documents and settings/ «utilisateur» /Windows** »).

Copyright ASIP Santé 2011. Tous droits réservés.

Il faudra alors, recopier tous ces fichiers (à l'exception du galss.ini et cps_pkcs11_safe.ini) dans le répertoire Windows (« **C:/Windows** » par défaut).

Remarque 2 : dans le cas d'une installation Cryptolib CPS GALSS avec un lecteur bi-fente sur port USB avec émulation port série virtuel (driver USB <-> COM), il sera préférable d'installer le driver USB/série sur le serveur, pour effectuer ensuite une redirection du périphérique USB du client vers le serveur. (Une redirection série s'un port COM virtuel peut poser problème dans certains cas)

3.2 Vérification du bon fonctionnement de la cryptolib

Lancer l'application CPSGestion (« cpgesw32.exe »).

Les données de la carte insérée seront affichées à l'écran, si l'installation s'est bien déroulée.

3.3 Paramétrage

1/ Chaque utilisateur du service TSE (ou surcouche CITRIX) devra donc avoir dans son répertoire personnel /Windows, un fichier **galss.ini**.

De ce fait, le fichier de configuration **galss.ini**, n'est pas propre au poste physique, mais au compte utilisateur.

Pour une utilisation des comptes utilisateur de manière nomade et avec des configurations de poste hétérogènes (ayant des configurations de lecteurs différentes), il faudra manuellement importer, à chaque ouverture de session, un fichier galss.ini correspondant à la configuration des lecteurs du poste.

A l'aide par exemple d'un script d'ouverture de session, qui recopiera le bon galss.ini, en fonction du poste client (voir l'administration de l'Active Directory du domaine réseau).

2/ Version GALSS : chaque utilisateur TSE/CITRIX, devra avoir les droits en écriture sur le répertoire :

« C:/Documents and settings/all users/santesocial/Coffre »

(Le fichier de cache « ccert.bin » doit pouvoir être modifié à tout moment par la Cryptolib CPS)

Copyright ASIP Santé 2011. Tous droits réservés.

3/ Configurer la redirection des lecteurs de carte du poste client vers le serveur, en fonction de leur type :

- **lecteur PSS série** : cocher l'option port série des options TSE (connexion TSE), et lancer la commande « **net use com1 : \\client\com1** » (connexion ICA CITRIX)

- **lecteur PC/SC** : cocher l'option « lecteur de cartes à puce » dans ressources locales (connexion TSE).

Copyright ASIP Santé 2011. Tous droits réservés.

4 Description de l'installation (version PC/SC)

Pour la version PC/SC, et en environnement client/serveur, aucune manipulation particulière n'est nécessaire (pas de GALSS installé).

4.1 Déroulement

Vous devez être administrateur du serveur, avant de démarrer la procédure.

1/ Lancer le setup d'installation de la Cryptolib CPS PC/SC pour Windows.

Suivre ensuite, le déroulement de l'installation comme indiqué dans le manuel d'installation standard de la Cryptolib CPS PC/SC.

2/ Lancer l'application CPSGestion (« **cpgesw32.exe** »).

Les données de la carte insérée seront affichées à l'écran, si l'installation s'est bien déroulée.

4.2 Paramétrage

La version PC/SC de la Cryptolib CPS gère en interne automatiquement les différentes configurations de poste (lecteurs de cartes), en cas de nomadisme des comptes utilisateur.

Donc, aucune configuration particulière des comptes utilisateur n'est nécessaire.

Seule la redirection des lecteurs PC/SC de cartes à puce du poste client vers le serveur, devra être activée. (Cocher l'option « lecteur de cartes à puce » dans ressources locales)

Copyright ASIP Santé 2011. Tous droits réservés.

5 Emplacements des fichiers

Ci-dessous, le résumé des emplacements des fichiers de la cryptolib, dans un environnement Client/serveur.

5.1 Chemin d'accès profil utilisateur [USER]

En fonction du système d'exploitation hôte, et du paramétrage des comptes utilisateurs, le chemin d'accès au profil utilisateur peut être différent :

1/ Par défaut en local :

Windows 2003 : [USER] = C:/documents and settings/ «utilisateur» /

Windows 2008 : [USER] : C:/utilisateurs/ «utilisateur» /

(Ou C:/users/«utilisateur» /)

2 / Par profil itinérant à distance :

Si des profils itinérants ont été définis, ces profils utilisateurs peuvent être stockés sur un partage réseau à distance.

Deux façons de gérer ces emplacements :

- depuis l'Active Directory du contrôleur de domaine -> users -> propriété d'un utilisateur -> profil -> chemin du profil

- à partir de GPO = stratégies de groupes.

(Voir avec votre administrateur de domaine, pour plus de détails).

Dans ce cas, la résolution du path se fait ainsi (Windows 2003 et 2008 Server) :

[USER] = %HOMEDIR%%HOMEPATH%

Ou **%HOMEDIR%** et **%HOMEPATH%** sont deux variables d'environnement, définissant le chemin d'accès du profil utilisateur distant.

(Accessibles avec la commande SET en ligne de commandes DOS).

(Variables non définis, si les profils itinérants ne sont pas utilisés)

Copyright ASIP Santé 2011. Tous droits réservés.

5.2 Version GALSS

galss.ini	[USER]/Windows
cps_pkcs11_safe.ini	[USER]/Windows
galclw32.dll	[WINDOWS]
galinw32.dll	[WINDOWS]
galssw32.dll	[WINDOWS]
pssinw32.dll	[WINDOWS]
pcscw32.dll	[WINDOWS]
cpsw32.dll	[WINDOWS]
cptabw32.dll	[WINDOWS]
sscasw32.dll	[WINDOWS]
cpgesw32.exe	[WINDOWS]
dico-fr.gip	[WINDOWS]
cps_pkcs11_w32.dll	[WINDOWS]
cps_csp_w32.dll	[SYSTEM]
cps_csp_w32.sig	[SYSTEM]

5.3 Version PC/SC

cpsw32.dll	[SYSTEM]
cptabw32.dll	[SYSTEM]
cps_pkcs11_pcsc_w32.dll	[SYSTEM]
cps_csp_pcsc_w32.dll	[SYSTEM]

Copyright ASIP Santé 2011. Tous droits réservés.

6 Annexe

6.1 Commande « change user »

Modifie le paramétrage relatif au mappage du fichier .ini.

Syntaxe

change user {**/execute** | **/install** | **/query**}

Paramètres

/execute

Active le mappage du fichier .ini au répertoire de base. Il s'agit du paramètre par défaut.

/install

Désactive le mappage du fichier .ini au répertoire de base. Tous les fichiers .ini sont lus et enregistrés dans le répertoire système. Vous devez désactiver le mappage du fichier .ini lors de l'installation des applications sur un serveur Terminal Server.

/query

Affiche le paramétrage actuel relatif au mappage du fichier .ini.

/?

Affiche l'aide à l'invite de commandes.

Remarques

- Utilisez la commande **change user /install** avant d'installer une application, pour créer des fichiers .ini pour cette application dans le répertoire système. Ces fichiers servent de sources pour les fichiers .ini spécifiques aux utilisateurs. Après avoir installé l'application, utilisez la commande **change user /execute** pour revenir au mappage du fichier .ini standard.
- La première fois que vous exécutez l'application, celle-ci recherche ses fichiers .ini dans le répertoire de base. Si les fichiers .ini ne se trouvent pas dans le répertoire de base mais dans le répertoire système, ces fichiers sont copiés dans le répertoire de base par les services Terminal Server, garantissant ainsi que chaque utilisateur dispose d'une copie unique des fichiers .ini de l'application. Les nouveaux fichiers .ini sont créés dans le répertoire de base.
- Chaque utilisateur doit disposer d'une copie unique des fichiers .ini d'une application. Cela permet d'éviter les situations où différents utilisateurs possèdent des configurations d'applications incompatibles, par exemple, des répertoires par défaut ou des résolutions d'écran qui ne sont pas les mêmes.
- Lorsque le système est en mode Installation (**change user /install**), plusieurs événements se produisent : toutes les entrées du Registre créées sont masquées sous **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\TerminalServer\Install**. Les clés ajoutées à **HKEY_CURRENT_USER** sont copiées sous la clé **\SOFTWARE**, tandis que les clés**HKEY_LOCAL_MACHINE** sont copiées sous **\MACHINE**. Si l'application interroge le répertoire Windows en utilisant des appels système, comme **GetWindowsDirectory**, les services Terminal Server renvoient le répertoire *RacineSystème*. Si des entrées de fichier .ini sont ajoutées à l'aide d'appels système, comme **WritePrivateProfileString**, elles sont ajoutées aux fichiers .ini sous le répertoire *RacineSystème*.
- Lorsque le système revient en mode d'exécution (**change user /execute**), et que l'application tente de lire une entrée du Registre sous **HKEY_CURRENT_USER** qui n'existe pas, les services Terminal Server vérifient si une copie de la clé existe sous la clé **\TerminalServer\Install**. Si c'est le cas, les clés sont copiées à l'emplacement approprié sous **HKEY_CURRENT_USER**. Si l'application tente de lire un fichier

Copyright ASIP Santé 2011. Tous droits réservés.

.ini qui n'existe pas, les services Terminal Server recherchent ce fichier .ini sous la racine système. Si le fichier .ini se trouve à la racine système, il est copié dans le sous-répertoire \Windows du répertoire de base de l'utilisateur. Si l'application interroge le répertoire Windows, les services Terminal Server renvoient le sous-répertoire \Windows du répertoire de base de l'utilisateur.

- Lorsque vous ouvrez une session, les services Terminal Server vérifient si ses fichiers système .ini sont plus récents que les fichiers .ini qui se trouvent sur votre ordinateur. Si la version système est la plus récente, votre fichier .ini est soit remplacé soit fusionné avec cette version. Ceci dépend du fait que le bit INISYNC, 0x40, a été défini ou non pour ce fichier .ini. La version précédente de votre fichier .ini est renommée en Inifile.ctx. Si les valeurs du Registre du système sous la clé **TerminalServer****Install** sont plus récentes que la version située sous **HKEY_CURRENT_USER**, alors votre version des clés est supprimée et remplacée par les nouvelles clés situées sous **TerminalServer****Install**.

6.2 Commande « change port » (changer le port)

Répertorie ou modifie les mappages du port COM pour maintenir la compatibilité avec les applications MS-DOS.

Syntaxe

Change port [{portx=porty|/d portx|/query}]

Paramètres

portx=porty

Mappe le port COM x au port y.

/d portx

Supprime le mappage du port COM x.

/query

Affiche les mappages de port actuels.

/?

Affiche l'aide à l'invite de commandes.

Remarques

- La plupart des applications MS-DOS ne prennent en charge que les ports séries COM1 à COM4. La commande change port mappe un port série vers un autre numéro de port, permettant ainsi aux applications qui ne gèrent pas un nombre important de ports COM d'accéder au port série. Par exemple, pour mapper le port COM12 au port COM1, afin de le rendre utilisable par une application MS-DOS, tapez change port com12=com1. La modification de mappage ne fonctionne que pour la session en cours et n'est pas conservée lorsque vous fermez une session pour en ouvrir une nouvelle.
- Utilisez la commande change port sans paramètres pour afficher les ports COM disponibles et leurs mappages actuels.

Copyright ASIP Santé 2011. Tous droits réservés.